CLAIMS

1. A method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name, comprising:
   (a) on a graphic user interface, displaying a name conflict indicator next to a first and a second display name, which display names are associated with different identities and are equivalent;
   (b) in response to a selection of a display name with a name conflict indicator displayed next thereto, displaying all display names that are equivalent to the selected display name; and
   (c) providing a mechanism to resolve the name conflict between two conflicting display names.

2. The method of claim 1 wherein step (a) comprises computing a clean name from each display name and comparing clean names of two display names to determine if the two display names are equivalent.

3. The method of claim 1 wherein each contact identity has an authentication level associated therewith and wherein step (a) comprises:
   (a1) examining the authentication levels of all display names that are equivalent; and
   (a2) displaying name conflict indicators next to selected display names based on the examination in step (a1).

4. The method of claim 3 wherein step (a2) comprises displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display names or (2) equals the highest

authentication/certification level to which at least two contact identities with equivalent display names have equal authentication levels.

5. The method of claim 3 further comprising:

(d) providing a security policy that determines the behavior of the collaboration system regarding communications with a contact based on the authentication level of that contact.

6. The method of claim 5 wherein step (d) comprises allowing a user of the collaboration system to determine the security policy.

7. The method of claim 5 wherein step (d) comprises allowing a system administrator to determine the security policy.

8. The method of claim 5 further comprising:

(e) warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

9. The method of claim 5 further comprising:

(e) preventing a user from communicating with another user based on the security policy when the other user has a predetermined authentication level.

10. The method of claim 1 wherein step (b) comprises displaying a dialog box having all display names that are equivalent to the selected display name listed therein.

11. The method of claim 1 wherein step (c) comprises assigning an alias to one of the first and second display names which alias is not equivalent to either of the first and second display names and which alias replaces the one display name.

12. The method of claim 1 further comprising:

(d) displaying an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

13. The method of claim 12 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

14. A method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, comprising:

(a) setting a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

(b) in response to an attempt by a user to communicate with one or more contacts, compiling a list of unauthenticated and uncertified contacts with whom the user is attempting to communicate; and

(c) warning the user and restricting the user from communicating with contacts with an unauthenticated and uncertified level based on the security policy.

15. The method of claim 14 wherein step (a) comprises a user setting the security policy that applies to that user.

16. The method of claim 14 wherein step (a) comprises a system administrator setting a security policy that applies to a user.

17. The method of claim 14 wherein step (c) comprises warning a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

18. The method of claim 14 wherein step (c) comprises preventing a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

19. The method of claim 14 wherein step (c) comprises allowing a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

20. The method of claim 14 wherein step (b) comprises:

(b1) compiling a contact list of contacts with whom the user is attempting to communicate;

(b2) checking the contact list to determine contacts that are not authenticated;

(b3) checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and

(b4) placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

21. Apparatus for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name, comprising:

means for displaying on a graphic user interface, a name conflict indicator next to a first and a second display name, which display names are associated with different contact identities and are equivalent;

means responsive to a selection of a display name with a name conflict indicator displayed next thereto for displaying all display names that are equivalent to the selected display name; and

a mechanism that resolves the name conflict between two conflicting display names.

22. The apparatus of claim 21 wherein the means for displaying a name conflict indicator comprises a mechanism that computes a clean name from each display name and a comparator that compares the clean names of two display names to determine if the two display names are equivalent.

23. The apparatus of claim 21 wherein each contact identity has an authentication level associated therewith and wherein the means for displaying a name conflict indicator comprises:

means for examining the authentication levels of all display names that are equivalent; and

means for displaying name conflict indicators next to selected display names based on display names that are determined to be equivalent by the means for examining the authentication levels.

24. The apparatus of claim 23 wherein the means for displaying name conflict indicators next to selected display names comprises means for displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display names or (2) equals the highest authentication/certification level to which at least two contact identities with equivalent display names have equal authentication levels.

25. The apparatus of claim 23 further comprising:

a mechanism that provides a security policy that determines the behavior of the collaboration system regarding communications with a contact based on the authentication level of that contact.

26. The apparatus of claim 25 wherein a mechanism that provides the security policy comprises a mechanism that allows a user of the collaboration system to determine the security policy.

27. The apparatus of claim 25 wherein the mechanism that provides the security policy comprises a mechanism that allows a system administrator to determine the security policy.

28. The apparatus of claim 25 further comprising:

a mechanism that warns a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

29. The apparatus of claim 25 further comprising:

a mechanism that prevents a user from communicating with another user based on the security policy when the other user has a predetermined authentication level.

30. The apparatus of claim 21 wherein the means for displaying all display names that are equivalent to the selected display name comprises means for displaying a dialog box having all display names that are equivalent to the selected display name listed therein.

31. The apparatus of claim 21 wherein the a mechanism that resolves the name conflict comprises a mechanism for assigning an alias to one of the first and

second display names which alias is not equivalent to either of the first and second display names and which alias replaces the one display name.

32. The apparatus of claim 21 further comprising:

a mechanism that displays an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

33. The apparatus of claim 32 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

34. Apparatus for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, comprising:

a mechanism that sets a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

means responsive to an attempt by a user to communicate with one or more contacts for compiling a list of unauthenticated and uncertified contacts with whom the user is attempting to communicate; and

a mechanism that warns the user and restricts the user from communicating with contacts with an unauthenticated and uncertified level based on the security policy.

35. The apparatus of claim 34 wherein the mechanism that sets the security policy comprises a mechanism that allows a user to set the security policy that applies to that user.

36. The apparatus of claim 34 wherein the mechanism that sets the security policy comprises a mechanism that allows a system administrator to set a security policy that applies to a user.

37. The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that warns a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

38. The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that prevents a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

39. The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that allows a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

40. The apparatus of claim 34 wherein the means for compiling a list of unauthenticated and uncertified contacts comprises:

means for compiling a contact list of contacts with whom the user is attempting to communicate;

means for checking the contact list to determine contacts that are not authenticated;

means for checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and

means for placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

41. A computer program product for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for displaying on a graphic user interface a name conflict indicator next to a first and a second display name, which display names are associated with different contact identities and are equivalent;

program code operable in response to a selection of a display name with a name conflict indicator displayed next thereto, for displaying all display names that are equivalent to the selected display name; and

program code that provides a mechanism to resolve the name conflict between two conflicting display names.

42. A computer program product for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for setting a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

program code operable in response to an attempt by a user to communicate with one or more contacts, for compiling a list of unauthenticated and uncertified contacts with whom the user is attempting to communicate; and

program code for warning the user and restricting the user from communicating with contacts with an unauthenticated and uncertified level based on the security policy.